ABSTRACT

Methods and apparati are provided for determining a "Squared Tate pairing" for hyperelliptic curves and using the results so support at least one cryptographic process. The improved techniques provide increased efficiency and an alternative method to the conventional method of implementing the Tate pairing for Jacobians of hyperelliptic curves. With the Squared Tate pairing for hyperelliptic curves, one may obtain a significant speed-up over a contemporary implementation of the Tate pairing for hyperelliptic curves. The Squared Tate pairing for hyperelliptic curves can be substituted for the Tate pairing for hyperelliptic curves in any applicable cryptographic application.